International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Advancement in Biometrics by Incorporating Inexorable Human Features

Parag P Chinawale[1], Prashant Y Itankar[2]

[1]Student, Computer Engineering Department, Mumbai University, Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India
[2]Assistant Professor, Computer Engineering Department, Mumbai University, Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India

---

Abstract - *As there is vigorous growth in technology and the necessity of providing security to data, there is also an increase in risk for the safety of these data from extortion. This research paper presents how the future advancement can be done in biometrics using the different hardware combined with Artificial Intelligence and machine learning, which will define the access based on human facial expressions and heart rate making sure that the person is in a free state of mind without any stress in the current situation.*

***Key Words*: Multi-Biometric system, recognition, authentication, inexorable human behaviour detection.**

1. INTRODUCTION

Clive Humby stated that "data is the new oil", after that economist published a report in 2017 titled "The **world's most valuable resource is no longer oil, but data**". From the very moment security towards data became the top priority and resulted in the use of biometrics as an advance feature for providing security. As there came new security there also came threats and drawbacks to it, like system may allow access by faking fingerprint, for face recognition if the photo of person was placed before sensor it allows access sometimes, but these drawbacks were overcome. As there is a new security there always comes some chances of the system to backlog. [1] Biometric refers to science of involving the statistical analysis of biological characteristics but, in today's world analysis of biological characteristics like fingerprint or face recognition is not enough. Many of the times it may happen that the person is being extorted for the data and unwillingly he/she has to leak data to someone who is extorting them. Situations like this can be overcome by using biometrics along with the analysis of inexorable(unavoidable) human behaviour in that current situation.

According to the 2017 Global Biometric Technology, market size was valued USD 14.40 billion, creating the scope of advancement in biometric technologies. The biometric aspect used as security are face, fingerprint, palm, voice, veins, signature etc.

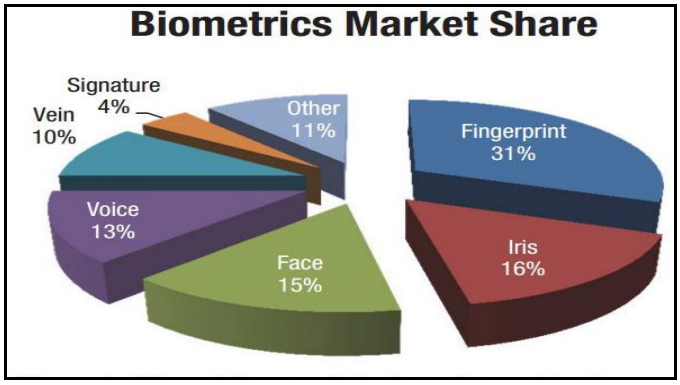


Chart-1: Biometric Market Usage

In the figure, we can see that the most used biometric system is fingerprint and iris recognition.The market using biometric as a security system has noted major 2 drawbacks

1. Biometric can be accessed by everyone: Your body aspects used as biometric like face, fingerprint, facial organs like eyes, ears, nose are open to all from which a dummy simulation can be created of one's biometric security. Voice can get recorded when anyone is talking.
2. Biometrics can get hackable: When Apple's iPhone was released with the fingerprint as biometric and was considered as the world's best security system, the very next day the hacker Jan Krissler was able to beat the technology. Similarly, researchers from the Chaos Computer Club created fake fingers to unlock iPhones. As there is a need to make it more secure.

As with the introduction to biometric, the "Safety lockers" were made which will unlock with biometrics. As these have an independent system without having the remotely situated database, the only way to open is to unlock it with owners biometric. This resulted in life threat of the owner. Many companies having sensitive data priority, which demanded the dual verification system. Also, the hacking techniques like spoofing takes more time to hack a system, as more than one biometric template or data need to be hacked and imitate in the system. Keeping this point in focus the further system is created by combining multiple physiological behavioural characteristics.

In this section, we will see the overview of the existing biometric systems like facial recognition and fingerprint. We will also see about the technologies which can be combine with these biometric systems for better security.

2. FINGERPRINT RECOGNITION

According to current studies and researches, there is a great successful advancement in the field of image processing and biometric authentication system based on two modes:

Enrolment and Recognition.[3] In the enrolment mode, the biometric data is acquired from the sensor and stored in a database along with the person's identity for the recognition. In the recognition mode, the biometric data is re-acquired from the sensor and compared to the stored data to determine the user identity.

The fingerprint recognition works as follows:

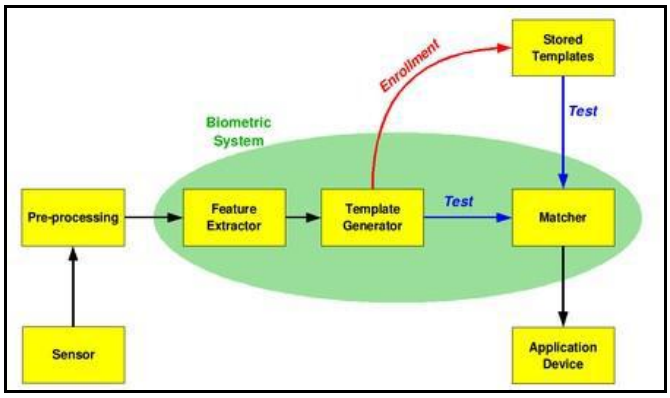


Chart-2: Fingerprint recognition block diagram

In this figure [4] we see, that how the fingerprint recognition system works form the start of enrolment, identification, and then verification.

In accordance with technologies using biometric aspects as a finger, there also exists the technology of counting heart rate using a fingertip. [5] This is done by first Pulse detection -> Signal extraction -> Signal amplification -> Physical properties. The block diagram of this mechanism is as follows:

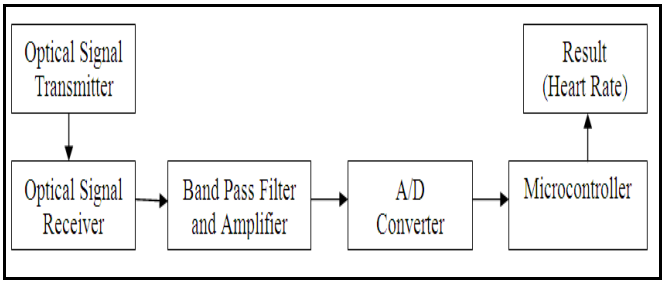


Chart- 3: Heart Rate system

The average resting human heart rate is about 70 bpm for adult males and 75 bpm for adult females. Heart rate varies significantly between individuals based on fitness, age, and genetics. Whenever a human body is under stress or any unwilling condition the pulse rate of the human body. Due to increase an in-heart rate, it becomes clear that the person is not in a stable nature.

Considering these technologies, a system can be created integrating the fingerprint and HRM system which will ensure that the access of those sensitive by the person is done under the free state. This can be done by combining these two systems.

According to the "American Heart Association", the heart rate of the human body according to the age is as follows:

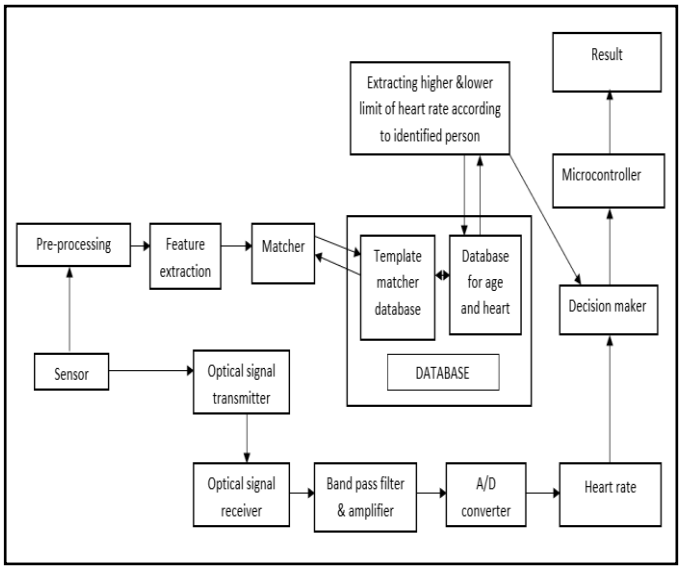
AGE	Target HR Zone 50-85%	Average Maximum Heart Rate,100%
20 years	100-170 beats per minute(bpm)	200 bpm
30 years	95-162 bpm	190 bpm
35 years	93-157 bpm	185 bpm
40 years	90-153 bpm	180 bpm
45 years	88-149 bpm	175 bpm
50 years	85-154 bpm	170 bpm
55 years	83-140 bpm	165 bpm
60 years	80-136 bpm	160 bpm
65 years	78-132 bpm	155 bpm
60 years	75-128 bpm	150 bpm

Chart-4: Heart Rate chart

By considering this, the limit of heart rate can be set for a person according to age. This will make sure the person's body fitness and mind in stable or stress-free conditions.

Then proposed combine system's block diagram is as followed:

Chart-5: Fingerprint and heart rate system



As given in the above block diagram, the sensor is the first prime component from which the pre-processing will begin from the data acquired from the sensor. The feature extractor extract's the features and creates a template and sends it to the matcher. The matcher is connected to the database, which have a stored template for verification. As the person is identified the heart rate limit corresponding to his/her as is extracted. Simultaneously the process for heart rate detection is started. The sensor uses an optical transmitter and receiver as the heart rate is calculated by the increase or decrease of density in blood using a photodiode. The amplifier is used to amplify and remove the distortion of the signal, it is done for the microcontroller to get proper frequency data. The A/D converter is used to convert analog signals to digital signals. Once the heart rate is converted to numerical format i.e. in digital number then it can be compared with the appropriate heart rate stored in a database. After this, the control is given to the microcontroller for handling the display and display drivers. Finally, the result gives if the access is granted or denied.

3. FACIAL RECOGNITION

Facial recognition is the most widely accepted form of biometric security system. Because of its accuracy in security, many changes were made in its architecture for its betterment. In earlier, they used various types of basic facial features that can be used for recognition by the system. There were 21 such features which included the hair color and width and thickness of lips. later on, it was noticed that the system allowed access even if the person's photo was placed in front of the camera sensor. In the starting year of 2010, Facebook started implementing the facial recognition system for the identification of its users' profile and identify the people in the photos that were updated by the user on a regular basis. In 2017, iPhone launched its phone model iPhone X, which had facial recognition as a primary security system that was widely accepted by the world. Apple made it public that it uses 30,000 projection points for facial recognition.

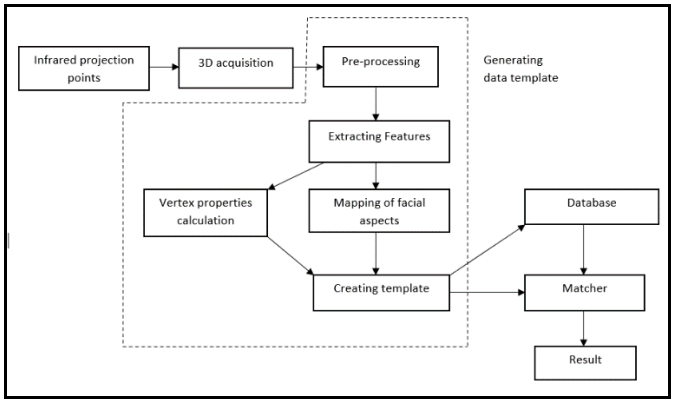


Chart-6: 3D face recognition system

In the above figure, we can see the flow of the real-time 3D facial recognition system. The basic element is the infrared projection points are placed on the face. Every time the location of each projection point is the same and set default. After the points are recorded, an image is formed and 3D acquisition is created. 3D data acquisition is rebuilding the 3D facial model from the data acquired form the data sensor. The needed information is further pre-processed. The information is extracted, and majorly 2 aspects are covered i.e. vertex properties calculation and mapping for facial aspects. Vertex properties calculation consists of the depth and angular calculation of nose to cheeks bone vertex, technically known as R-Orbital Lower and L-Orbital Lower. The mapping of facial aspect includes aspects like height between upper and lower lips, between lower lip and chin, the width of lips, upper and lower eyelid, width of eyes, distance between eyes, and many more aspects. After this, a mathematical expression is created from this data and stored in the database. Whenever a face is placed in Infront of the sensor this process is repeated, and atlas the mathematical equation created is compared with the mathematical expression stored in the database, this is done by matcher and the result is displayed.The same related technology which uses facial aspect as a major part of its system is recognition of facial expression.

Facial expression recognition software is a technology that uses various facial aspects to detect the emotion. Majorly it is the technology which uses the data and analyses the reaction on the face. It includes the six basic or universal expressions: happiness, sadness, anger, surprise, fear, and disgust. In this image processing is done to get the important or to extract needed features from the image. Many companies like Google, Microsoft and Amazon have their own API for this function. This is detected by mapping certain features like exact corner of eye, detection of eye region, detection of

eyebrow region, detection of mouth region. The changes in these regions are taken into consideration like upper and lower lids of eyes, corner of eyebrows, lip corner, change in upper and lower lips. Further a confusion matrix is created for more accuracy for facial recognition. Each feature is stored in vector format, the current image vector is matched with the stored or predefined vector.

Emotions	Services			Average
	Amazon	Google	Microsoft	
Anger	42%	45%	90%	**59%**
Happiness	100%	100%	100%	**100%**
Sadness	81%	95%	97%	**91%**
Surprise	91%	99%	99%	**96%**
Average	**79%**	**85%**	**97%**	

Chart-7: Expression recognition accuracy comparison

After studying the detail about the API, [6] we come to a result that Microsoft has the accuracy of 97% followed up by Google API by 85% and amazon by 79%.

By combining these two technologies a more secure system can be created. This can be done by first performing the facial unlock system and simultaneously performing and only if the person is in neutral or in the happy state then only the access will be granted. If the person is in a sad or angry state it can be a threat to the piece of information or anything being accessed. The flow of the is as followed:

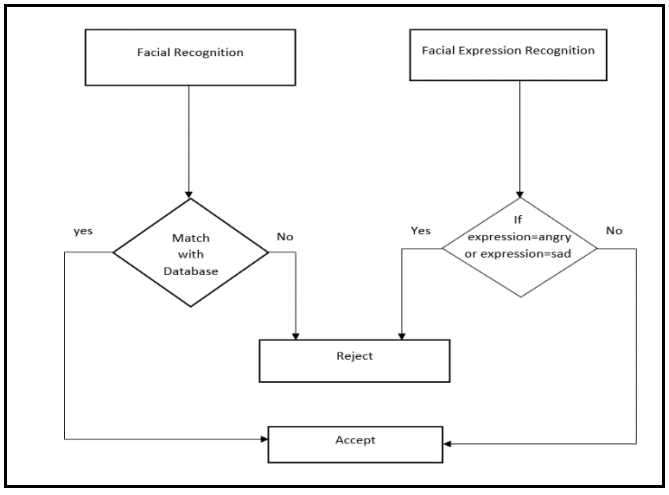


Chart-8: System flow diagram of facial recognition and expression

As shown in the above algorithm, once the face is recognized simultaneously the facial expression is also recognized. The decision is made based on the expression detected. For both the conditions satisfy i.e. the face matches with the template stored in the database and the expression is also acceptable then only the access is granted or else access it is rejected.

4. RELATED WORK

The system for that would make biometric more secure was the main aim and the biometric system having multiple biometric was defined. This was done by using two biometric system by detection both the biometric aspect and if both matches, then only access is to be granted [4].

Facial recognition [8] development is done by using different language and detail study is done. The simulation and practical can be performed by using MATLAB language, real-time prototype systems were designed and developed [7].

Emotions on the face are recognisable by using image processing and by its detail study [9]. The advancement is done by many companies like Google, Microsoft and Amazon.

This leads to the competition of creating more accuracy in facial expression recognition system, which is decided by comparing various API's and the accuracy of those API's to recognise facial expression [6].

5. CONCLUSION

Security has got a new face since biometric system was introduces. It provides a valuable scope of advancement in the field of security. But in the digital era, using single physiological aspect is not enough. This paper provides the solution by combining the physiological aspect with the current body condition making the system less vulnerable and more secure. Even though the facial expression recognition technology is not totally developed, there is still a wide range of scope for it. As many of physiological aspects are live which means that they are not stored like heart rate and expression is becomes time consuming and the system less vulnerable.

REFERENCES

[1] Marcos Faundez-Zanuy," Biometric security technology," Escola Universitaria Politècnica de Mataró Avda. Puig I Cadafalch 101-111 08303 MATARO (BARCELONA) SPAIN.

[2] Abdulmonam Omar Alaswad, Ahlal H. Montaser, Fawzia Elhashmi Mohamad," Vulnerabilities of Biometric Authentication "Threats and Countermeasures"," International Journal of Information & Computation Technology.

ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958

[3] Mouad .M.H.Ali, Vivek H. Mahale, Pravin Yannawar, A. T. Gaikwad on "Overview of Fingerprint Recognition

System", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[4] Sahana J , Tarun R, Manjunath C on " Multi Biometric Recognition System**",** International Journal of Computer Science and Mobile Computing, Vol.8 Issue.6, June- 2019, pg. 89-94

[5] M.M.A. Hashem, Rushdi Shams, Md. Abdul Kader, Md. Abu Sayed, "Design and Development of a Heart Rate Measuring Device using Fingertip," Department of Computer Science and Engineering Khulna University of Engineering & Technology (KUET) Khulna 9203, Bangladesh.

[6] Osamah M Al-Omair, Shihong Huang "A Comparative Study on Detection Accuracy of Cloud Based Emotion Recognition Services," Computer & Electrical Engineering and Computer Science Florida Atlantic University Boca Raton, FL 33431, USA

[7] M. Meenakshi, "Real-Time Facial Recognition System—Design, Implementation and Validation," doi:10.7726/jspta.2013.1001, January 2013

[8] Jozef Bushati, Virtyt Lesha, Dea Strica," THE MODELING OF FACIAL RECOGNITION PROCESS IN PROSPECTIVE OF SIMULATION TECHNIQUES (A methodical elaboration through the built-in modules of Matlab)," University of Shkodra, Shkodra; Albania Polytechnic University of Tirana, Tirana, Albania; University of Tirana, Tirana, Albania

[9] Paweł Tarnowski, Marcin Kołodziej, Andrzej Majkowski, Remigiusz J. Rak," Emotion recognition using facial expressions," International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland.